APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,433	02/06/2004	Marcus Leech	57983.000164	5978

7590   04/16/2009

Thomas E. Anderson
Hunton & Williams LLP
1900 K Street, N.W.
Washington, DC 20006-1109

EXAMINER
LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
04/16/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/772,433	LEECH, MARCUS
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2432	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>04 March 2009</u>.
2a) ☐ This action is **FINAL.**   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1 and 3-20</u> is/are pending in the application.
    4a) Of the above claim(s) <u>1 and 3-11</u> is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) <u>12-20</u> is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☐ All b) ☐ Some * c) ☐ None of:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
         application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)
1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1.　　　Claims 1, 3-11 are directed to an invention that is independent or distinct from the invention originally claimed because the claims are directed to the following patentably distinct species:

　　　　Species 1: Originally filed claim 5.

　　　　Species 2: Claims 1, 3-11.

2.　　　Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 1, 3-11 are withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

3.　　　Should applicant traverse on the ground that the species are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the species to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the species unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other species.

Response to Arguments

4.　　　Applicant's arguments regarding claims 1 and 3-11 have been considered but are moot in view of the claims being withdrawn from consideration.

5.　　　Applicant argues, "A concatenation operation is very different from an XOR operation in both form and result." In response, Applicant has misinterpreted the application of the reference. The summation of the XOR is meant to read on the claimed concatenation. The Examiner never

stated that the XOR operation itself was intended to meet the claimed concatenation, but instead

said that it was the XOR-**sum**.

6.   Applicant's argument that "combining Schneier with Rogaway…would result in an

inoperable methodology…" is not persuasive because Applicant has failed to provide any

evidence to support their allegation.

Claim Rejections - 35 USC § 101

7.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or
> any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
> requirements of this title.

8.   Claims 12-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed

to non-statutory subject matter. A claimed process is surely patent-eligible under § 101 if: (1) it

is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different

state or thing. See Benson, 409 U.S. at 70; Diehr, 450 at U.S. at 192; see also Flook, 437 U.S. at

589 n.9. The mere field-of-use limitations are generally insufficient to render an otherwise

ineligible process claim patent-eligible. See Diehr, 450 at U.S. at 191-92. In this case, the claims

are considered non-statutory because the claimed process is not tied to a particular machine or

apparatus.

Claim Rejections - 35 USC § 103

9.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

10.   The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness under 35

U.S.C. 103(a) are summarized as follows:

      1.   Determining the scope and contents of the prior art.
      2.   Ascertaining the differences between the prior art and the claims at issue.
      3.   Resolving the level of ordinary skill in the pertinent art.
      4.   Considering objective evidence present in the application indicating obviousness
          or nonobviousness.

11.   Claims 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rogaway,

in view of Schneier. Referring to claims 12, 20, Rogaway discloses that each message blocks is

concatenated (Page 5, checksum generation function), which meets the limitation of applying a

XOR function to all message blocks of a message to compute a XOR-sum. The checksum is then

XOR'd with $Z[m]$ (Page 5, calculation of value 'T'), which meets the limitation of applying a

third mask value to the XOR-sum. The result of the XOR function is then encrypted (Page 5,

calculation of value 'T'), which meets the limitation of encrypting the masked XOR-sum using

the block cipher and the first key. Rogaway does not disclose XOR'ing the result of the

encryption with a value. However, it would have been obvious to one of ordinary skill in the art

at the time the invention was made to XOR the data after the block algorithm, in addition to

before, because this technique is not susceptible to meet-in-the-middle attack as taught by

Schneier (Page 367).

      Referring to claim 13, Rogaway discloses that the corresponding block of the generated

value is generated based on the XOR of an encrypted nonce (Page 5, R) and an encrypted value

(Page 5, L), which meets the limitation of the first/third mask value is computed by applying a

XOR function to a first value derived from a nonce value and a second value derived from

encrypting a third value using the block cipher and a key, wherein the second/fourth mask value

is computed by applying a XOR function to a fourth value derived from the nonce value and a

fifth value derived from encrypting a sixth value using the block cipher and a key. Rogaway does

not specify that the key used to encrypt the value to generate the 'L' (Page 5) is different than the

key used to encrypt M[i] $\oplus$ Z[i] (Page 5). However, it would have been obvious to one of

ordinary skill in the art at the time the invention was made to use multiple keys in the encryption

algorithm in order to enhance the strength of the encryption algorithm by making the algorithm

more difficult to break. Using only a single encryption key is easier break than using multiple

because an attacker would only need to discover the one key as opposed to having to discover

every key that is used in the encryption algorithm. Rogaway also does not disclose applying a

substitution function to the result of the XOR function on L and R. However, it would have been

obvious to one of ordinary skill in the art at the time the invention was made to perform a

substitution function on the result of the XOR function on L and R because substitution

operations are an important part of block cipher algorithms that give them security as taught by

Schneier (Page 275).

Referring to claim 14, Rogaway discloses that to compute the R value, the nonce is

XOR'd with L and the result of the XOR function is encrypted with key K (Page 5), which meets

the limitation of the first and fourth values derived from the nonce value are permutations of a

binary value computed by encrypting the nonce value using the block cipher and the first key.

Referring to claims 15, 16, Rogaway discloses encrypting a message by exclusive or'ing

a block of the message with a corresponding block of a generated value (Page 5, M[i] $\oplus$ Z[i]),

which meets the limitation of whitening at least one message block with a third mask value. The

result of that exclusive or operation is encrypted (Page 5) using a block cipher (Page 4), which

meets the limitation of encrypting the at least one whitened message block using a block cipher

and a first key. The result of the encryption is the exclusive or'ed with a corresponding block of

the generated value (Page 5), which meets the limitation of whitening the at least one encrypted

message block with the third mask value to generate at least one corresponding output ciphertext

block.

Referring to claim 17, Rogaway discloses that the corresponding block of the generated

value is generated based on the XOR of an encrypted nonce (Page 5, R) and an encrypted value

(Page 5, L), which meets the limitation of the first and second mask values are computed by

applying a XOR function to a first value derived from a nonce value and a second value derived

from encrypting a third value using the block cipher and a key. Rogaway does not specify that

the key used to encrypt the value to generate the 'L' (Page 5) is different than the key used to

encrypt $M[i] \oplus Z[i]$ (Page 5). However, it would have been obvious to one of ordinary skill in

the art at the time the invention was made to use multiple keys in the encryption algorithm in

order to enhance the strength of the encryption algorithm by making the algorithm more difficult

to break. Using only a single encryption key is easier break than using multiple because an

attacker would only need to discover the one key as opposed to having to discover every key that

is used in the encryption algorithm. Rogaway also does not disclose applying a substitution

function to the result of the XOR function on L and R. However, it would have been obvious to

one of ordinary skill in the art at the time the invention was made to perform a substitution

function on the result of the XOR function on L and R because substitution operations are an

important part of block cipher algorithms that give them security as taught by Schneier (Page

275).

Referring to claim 18, Rogaway discloses that the block cipher used is the AES block

cipher (Page 6, first paragraph), which meets the limitation of the block cipher is AES.

Referring to claim 19, Rogaway discloses that the L and R values are elements of the

offset vector Z (page 5), which meets the limitation of the second and fifth values are elements of

a vector.

Conclusion

12.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-

3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432